Preparing for the New Wave of HIPAA Enforcement in 2016

Are you ready to navigate this dangerous minefield?

By Raymond F. Posa, MBA

Tips from the Trenches is a new every-issue column featuring practice management issues, and is written exclusively for PM by members of the Institute for Podiatric Excellence and Development (IPED). IPED’s mission is to motivate, inspire, and synergistically bridge the gap between students, residents, new practitioners, and seasoned veterans in the field of podiatric medicine. They are committed to the idea that mentors with passion to share and mentees eager to learn make a powerful combination that allows IPED to bring and renew a full life to podiatric physicians, their practices, and their well-being throughout the U.S. and beyond. Visit www.podiatricexcellence.org.

Government regulation and enforcement is a relentless juggernaut, and 2016 looks to be a very tough year for those practices that are not prepared. The Department of Health and Human Services (HHS) is under the gun from the US Senate to step up efforts to protect PHI. Last year saw the largest number of data breaches to date under the HIPAA legislation, and the Senate wants answers. It is HHS’s job now to turn the screws on the Office of Civil Rights (OCR) and the Center for Medicare and Medicaid Services (CMS).

As the Senate puts pressure on HHS, HHS in turn puts pressure on OCR and CMS. The HHS Office of Inspector General in September released its report, “OCR Should Strengthen Its Oversight of Covered Entities’ Compliance with the HIPAA Privacy Standards.” In its report, HHS makes five recommendations to OCR: 1) fully implement a permanent audit program; 2) maintain complete documentation of corrective action; 3) develop an efficient method in its case-tracking system to search for and track covered entities; 4) develop a policy requiring OCR staff to check whether covered entities have been previously investigated; and 5) continue to expand outreach and education efforts to covered entities.

Efforts have already begun in CMS and OCR to address these recommendations. Many of you may already be familiar with the auditing firm for CMS, Figliozzi & Company. Figliozzi’s contract is winding down and will be replaced with a new auditing contract that will go beyond “desk” audits which are done via email, and will begin on-site audits. CMS has learned a lot from the Meaningful Use Audit program, and the program has evolved over the last couple of years. It started out doing post-payment audits for years 2011 and 2012, and then it moved to pre-payment audits for 2013 and 2014, and now it is conducting what are known as Year 1 audits. The lessons learned were that covered entities were slow to the party and are just now making some efforts to get compliant. Knowing that and using the 6 year look-back period provided by HIPAA, they are now doing audits of the 2011 period. They realized that non-compliance was much higher then, and the first year stimulus payouts were highest then. This is Figliozzi’s opportunity to go out with a bang and recoup millions of dollars.

The other thing learned from Meaningful Use is that 80% of failures were due to poor or non-existent Risk Analysis Reports. You can bet that those failures will be part of OCR’s requirement to check if cov-

Continued on page 44
business associates, EMC Corporation, had to pay $90,000 to the state of Connecticut for the theft of an unencrypted laptop. During the investigation, it was also found that Hartford Hospital did not have a signed Business Associate Agreement with ECM.

The states and the federal government are taking violation of the HIPAA rules very seriously, and enforcement is getting tougher and more vigorous. The Privacy Rule was enacted in 2003 and the Security Rule in 2005. Compliance with these rules has now been deemed to be the new standard of care. Violations of these rules in several states have now resulted in civil action against covered entities. When the HIPAA rules were first enacted, there was never a pathway for civil action against a covered entity by a patient. That is changing, and soon all 50 states will have laws on the books allowing civil action against covered entities for breaches of PHI.

The best advice for covered entities is to take HIPAA compliance very seriously. You must have a comprehensive compliance plan in place. Your compliance officer must know the plan and implement it. The practice must live its compliance plan. Failure to do so can result in a $750,000 penalty as in the case of the University of Washington Medicine (UWM). OCR’s investigation found that UWM “failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of e-PHI”. Filling out on-line questionnaires by a staff member with no technical training is a sure fire way to fail an on-site audit. Your Risk Analysis must be thorough and competent in order to ensure that it is a credible effort.

Finally, have complex passwords been driving your staff crazy with changing your passwords every 90 days? Well, here comes more: two-factor authentication. ONC has put out a brief that makes reference to the DEA’s requirement to add two-factor authentication in the Electronic Prescription for Controlled Substances interim final rule in 2010.

If you would like a free compliance checklist or if you have any questions regarding your compliance plan, please feel free to contact me at (732) 919-0944 or email rposa@themantagroup.com.

**Filling out on-line questionnaires by a staff member with no technical training is a sure fire way to fail an on-site audit.**

---

Mr. Posa is President of The Mantag Group, a technology consulting firm in Farmingdale, NJ. Mr. Posa is a trustee on the Board of Directors of the American Academy of Podiatric Practice Management (AAPPM). He is the technology advisor to AAPPM and has achieved Fellow status with the AAPPM. He is a national speaker on technology and HIPAA issues, and has been published in various medical publications and websites. He can be reached at (732) 919-0944 or rposa@themantagroup.com.